

JACK P. DICANIO (SBN 138782)  
Jack.DiCanio@skadden.com  
EMILY REITMEIER (SBN 305512)  
Emily.Reitmeier@skadden.com  
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP  
525 University Avenue  
Palo Alto, California 94301  
Telephone: (650) 470-4500  
Facsimile: (650) 470-4570

MATTHEW E. SLOAN (SBN 165165)  
Matthew.Sloan@skadden.com  
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP  
300 South Grand Avenue, Suite 3400  
Los Angeles, California 90071-3144  
Telephone: (213) 687-5000

Yan Ge (SBN 236566)  
geyan@us.kwm.com  
KING & WOOD MALLESONS LLP  
535 Middlefield Road, Suite 245  
Menlo Park, CA 94025  
Telephone: (650) 858-1285

Aaron Wolfson (admitted *pro hac vice*)  
KING & WOOD MALLESONS LLP  
aaron.wolfson@us.kwm.com  
500 5th Ave #50  
New York, NY 10036  
Telephone: (212) 319-4755

Attorneys for Defendant  
FUJIAN JINHUA INTEGRATED CIRCUIT CO., LTD.

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

FUJIAN JINHUA INTEGRATED CIRCUIT  
CO., LTD., et al.,

Defendant.

Case No. 18-CR-465 MMC

**FUJIAN JINHUA INTEGRATED CIRCUIT  
CO., LTD.'S NOTICE OF MOTION AND  
MOTION IN LIMINE NO. 4 TO EXCLUDE  
THE FORENSIC IMAGES OF CERTAIN  
ELECTRONIC DEVICES;  
MEMORANDUM OF POINTS AND  
AUTHORITIES; DECLARATION OF  
MATTHEW E. SLOAN; [PROPOSED  
ORDER]**

Judge: The Honorable Maxine M. Chesney  
Trial Date: February 14, 2022  
Hearing Date: January 18, 2022  
Hearing Time: 10:00 a.m.

**NOTICE OF MOTION AND MOTION**

TO THE CLERK OF THE COURT, ALL PARTIES, AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on January 18, 2022 at 10:00 a.m., or as soon thereafter as the matter may be heard at a time set by The Honorable Maxine M. Chesney in Courtroom 7 of the United States District Court for the Northern District of California, located at 450 Golden Gate Avenue, San Francisco, California, defendant Fujian Jinhua Integrated Circuit Co., Ltd. (“Jinhua”), will move the Court to exclude the forensic images of certain electronic devices seized by the Taiwan authorities in February, 2017 and produced to Jinhua in discovery, on the grounds that the electronic data on these devices was accessed and modified before being forensically imaged, thus corrupting the integrity of the data (“Motion”). This Motion is based upon the Notice of Motion and Motion, Memorandum of Points and Authorities, the Declaration of Matthew E. Sloan (“Sloan Decl.”) and exhibits thereto, the pleadings and papers on file in this action, and such further arguments and matters as may be presented at the time of the hearing on this Motion.

## TABLE OF CONTENTS

1			
2	NOTICE OF MOTION AND MOTION .....	ii	
3	TABLE OF CONTENTS.....	iii	
4	TABLE OF AUTHORITIES .....	iv	
5	ISSUES TO BE DECIDED .....	1	
6	ARGUMENT AND AUTHORITIES.....	1	
7	I.    INTRODUCTION .....	1	
8	II.   STATEMENT OF FACTS .....	2	
9	A.    Taiwan Investigation and Indictment.....	2	
10	B.    DOJ’s Request for Mutual Legal Assistance and Transfer of		
11	Evidentiary Materials.....	5	
12	C.    Discovery of Alleged Trade Secrets on Forensic Image of Seized		
13	Devices.....	5	
14	III.  ARGUMENT.....	8	
15	A.    The Prosecution Has Not Produced Sufficient Evidence For A		
16	Reasonable Juror To Determine That The Devices Are In		
17	Substantially The Same Condition As When They Were Seized .....	9	
18	B.    The Taiwan MJIB Failed To Follow Proper Forensic Protocol In		
19	Searching The Seized Devices, Thereby Contaminating The Data		
20	That They Contain .....	11	
21	C.    The Government and its Taiwanese Counterpart Have Spoliated the		
22	Most Critical Evidence for Both the Prosecution and the Defense by		
23	Negligently Handling the Corrupted Devices Before Creating a		
24	Forensic Image.....	13	
25	1.    The significance of the information stored on the corrupted		
26	devices should have been obvious to the Taiwanese MJIB and		
27	they have acted in bad faith by deviating from the standard		
28	practice of immediately creating forensic images of the		
	electronic devices upon seizure. ....	14	
	2.    The Taiwanese authorities were at least negligent in deviating		
	from the established best practice of forensically imaging the		
	corrupted devices immediately after they were seized and		
	delivered to the MJIB Lab. ....	15	
	3.    The corrupted devices in their untampered original state		
	would have been the most relevant and crucial evidence on		
	the issue of whether alleged trade secret information were in		
	the possession of the defendants. ....	16	
	IV.   CONCLUSION.....	16	

## TABLE OF AUTHORITIES

### CASES

<i>Arizona v. Youngblood</i> , 488 U.S. 51, 109 S. Ct. 333 (1988).....	14
<i>California v. Trombetta</i> , 467 U.S. 479, 104 S. Ct. 2528 (1984).....	13, 14
<i>Caruso v. Solorio</i> No. 115CV780AWIEPGPC, 2021 WL 3514610 (E.D. Cal. Aug. 10, 2021).....	14
<i>Gates Rubber Co. v. Bando Chemical Indus., Ltd.</i> 167 F.R.D. 90 (D. Colo. 1996).....	14
<i>Glover v. BC Corp.</i> , 6 F.3d 1318 (9th Cir. 1993).....	12, 15
<i>Nova Measuring Instruments Ltd. v. Nanometrics, Inc.</i> , 417 F. Supp. 2d 1121 (N.D. Cal. 2006).....	15
<i>Singleton v. Kernan</i> , No. 3:16-CV-2462-BAS-NLS, 2018 WL 5761688 (S.D. Cal. Nov. 1, 2018).....	13
<i>Unigard Sec. Ins. Co. v. Lakewood Eng'g &amp; Mfg. Corp.</i> , 982 F.2d 363 (9th Cir. 1992).....	13, 16
<i>United States v. Ganias</i> , 824 F.3d 199 (2d Cir. 2016).....	12
<i>United States v. Godoy</i> , 528 F.2d 281 (9th Cir. 1975).....	9
<i>United States v. Hock Chee Koo</i> , 770 F. Supp. 2d 1115 (D. Or. 2011).....	9, 11, 13
<i>United States v. Kimoto</i> , 588 F.3d 464 (7th Cir. 2009).....	12
<i>United States v. Maxxam, Inc.</i> , No. C-06-07497CWJCS, 2009 WL 817264 (N.D. Cal. Mar. 27, 2009).....	13
<i>United States v. Panero</i> , 266 F.3d 939 (9th Cir. 2001).....	9
<i>United States v. Rodriguez</i> , No. 16-CR-41G, 2018 WL 947266 (W.D.N.Y. Feb. 20, 2018).....	11, 14, 15
<i>United States v. Safeco Ins. Co. of Am.</i> , No. 3:14-CV-00190-BLW, 2016 WL 901608 (D. Idaho Mar. 9, 2016).....	13
<i>United States v. Salcido</i> , 506 F.3d 729 (9th Cir. 2007).....	9
<i>In re Vioxx Prod. Liab. Litig.</i> , No. MDL 1657, 2005 WL 756742 (E.D. La. Feb. 18, 2005).....	15

1 **STATUTES, RULES & REGULATIONS**

2 Federal Rules of Evidence 104(a)..... 1  
3 Federal Rules of Evidence Rule 901(a)..... 1, 6, 7

4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ISSUES TO BE DECIDED**

Defendant Jinhua seeks an Order from the Court excluding the forensic image of certain electronic devices that were seized by the Taiwan authorities in raids on United Microelectronics Corporation (“UMC”) in February 2017 on the grounds that they were accessed and modified before being forensically imaged.

**ARGUMENT AND AUTHORITIES****I. INTRODUCTION**

Fujian Jinhua Integrated Circuit Co., Ltd. (“Jinhua”) respectfully submits this Memorandum of Law in support of its motion in *limine* to exclude certain electronic information from being admitted into evidence. Specifically, Jinhua seeks to exclude the forensic image of certain electronic devices that were seized by the Taiwan authorities in raids on United Microelectronics Corporation (“UMC”) in February 2017 on the grounds that they were accessed and modified before being forensically imaged. Given the extent to which the seized devices were altered, any forensic image captured following such alteration cannot accurately represent the data stored on these devices at the time of their seizure, and the government will not be able to satisfy its burden of authentication under Rule 901 of the Federal Rules of Evidence. Allowing the government to introduce these forensic images into evidence would unfairly prejudice Jinhua, which would be forced to challenge the existence of alleged trade secret information based on spoliated evidence. Accordingly, the Court should exclude the forensic image.

The government should not be allowed to build its case on the basis of data collected from electronic devices that have been subject to significant post-seizure tampering and manipulation, and certainly not to show that these devices contain misappropriated trade secret information at the time they were seized. In short, the government’s entire case hinges upon the contents of the devices that it carelessly handled and spoliated.

After seizing 26 devices that the Taiwanese authorities suspected of containing misappropriated trade secret information, the prosecutors and investigators did not make any effort to preserve the status quo of the seized digital media. Rather, they not only accessed and reviewed the existing files on the devices, but also created and downloaded additional files while also deleting

certain files. To make matters worse, the Taiwanese authorities invited an employee of Micron Memory Taiwan Co., Ltd. (“MMT”), the company that filed the initial criminal complaint in Taiwan and stood to benefit from charges being brought against UMC and Jinhua, to review the seized devices before they were forensically imaged.

The Taiwanese authorities’ disregard for the integrity of the evidence and deviation from established best practices in handling the digital forensic investigation process have destroyed any chance of establishing the authenticity of the data stored in the devices. Thousands of files were created, altered, or deleted post-seizure, substantially changing the condition of the devices. As such, the devices can no longer be authenticated and should be excluded from the evidence to be presented at trial.

## II. STATEMENT OF FACTS

### A. Taiwan Investigation and Indictment

Acting on a criminal complaint from MMT and its parent, Micron Technology, Inc. (“Micron”) in September 2016, the Taiwan Ministry of Justice Investigation Bureau (“MJIB”), New Taipei Branch, led by prosecutors of the Taiwan Taichung District Prosecutors Office, searched UMC’s facilities and seized a total of 26 electronic devices from UMC employees between February 7 and 14, 2017. Sloan Decl., Ex. A (Indictment Decision of Taiwan Taichung District Prosecutors Office (“Taiwan Indictment”)) at 7, 17.

The devices were eventually delivered to the MJIB Forensics Laboratory (the “MJIB Lab”) for forensic examination. Sloan Decl., Ex. B (a brief description provided by Lewei Chen (“Chen Description”)) at 1. However, instead of following the standard practice of creating a forensic mirror image of the digital media immediately following seizure so as to preserve their contents, the Taiwanese authorities contaminated and altered data and metadata present on the storage media in the seized devices by performing searches and otherwise accessing almost half of the seized devices.

Specifically, as demonstrated by the expert report of Jinhua’s forensic evidence expert, John Ashley, the Managing Director of Consilio’s Digital Forensics and Expert Services Department,<sup>1</sup> the

<sup>1</sup> As Mr. Ashely’s curriculum vitae establishes, Mr. Ashely is a leading expert in the forensic examination field with over thirty years of experience. See Ex. G (Ashley Report), Ex. 1 (Curriculum

Taiwanese authorities accessed and searched the various laptops, USB devices and hard drives seized from UMC employees on multiple occasions before creating forensic images of the devices. As a result, the data stored on the following 10 devices (the “corrupted devices”) was altered or deleted after the devices were seized but before they were imaged:

1. **Device 106030-25-03 (BRG003)<sup>2</sup> Intel 240GB UMC Laptop drive:** Laptop **106030-25-03**, which the Taiwan authorities identified as a laptop used by defendant Kenny Wang, Sloan Decl., Ex. C (Explanation Regarding Evidence Transfer of Taichung District Prosecutors’ Office of Taiwan on March 16, 2020 A.D. (“Evidence Transfer Explanation”)) at 4. This laptop was seized on February 7, 2017 by the MJIB and was accessed multiple times on February 7, 8, 13, and 17, 2017 before being forensically imaged on February 20, 2017. Almost 35,000 files were added to the drive in this laptop and more than 1,000 files were deleted. Of the files and folders added, 32,688 were copied from the UMC server \\p58f21\Data\NBD on 2/7/2017. Multiple USB devices have also been attached to the laptop on that date. The MJIB activity added 13.38 Gigabytes of data to the drive. Moreover, Yi-Leng Chen, an MMT employee, accessed the laptop and performed a review on February 13, 2017 from 11:25 until 19:25. Sloan Decl., Ex. G (Expert Witness Disclosure of John F. Ashley (“Ashley Report”)) at 10.
2. **106030-25-04 (BRG004) SanDisk Cruzer Edge 8GB USB disk:** USB disk **106030-25-04**, seized on February 7, 2017, was accessed on February 17, 2017 before being forensically imaged on February 20, 2017. 93 files and 5 folders were created on the USB drive on February 17, 2017. *Id.* at 11.
3. **106030-25-06 (BRG006) Rundisk 1GB USB drive:** USB disk **106030-25-06**, which was seized on February 7, 2017, was accessed on February 13, 2017 before being forensically imaged on February 20, 2017. *Id.* at 12. MMT employee Yi-Leng Chen accessed the USB device on February 13, 2017 from 11:25 to 19:25 and reviewed files and folders on the device. *Id.*
4. **106030-25-09 (BRG009) Western Digital 250GB drive from Acer Laptop:** Laptop **106030-25-09**, seized on February 7, 2017, was accessed on February 7 and 13, 2017 before being forensically imaged on February 20, 2017. *Id.* at 13-14. Five separate USB devices were inserted into this laptop when it was accessed on February 7 after seizure. *Id.* More than 4,500 files and folders had their metadata details altered with a number of files being added to or deleted from the laptop. *Id.* at 14. MMT employee Yi-Leng Chen accessed the laptop on February 13, 2017 from 11:25 to 19:25 and reviewed files and folders on the device. *Id.*
5. **106030-25-11 (BRG011) Transcend 1TB USB drive:** USB disk **106030-25-11**, seized on February 8, 2017, was accessed on February 13, 2017 before

Vitae). Among other things, Mr. Ashley was formerly the Chief of the Greater Manchester Police Department’s Computer Examination Unit (which at the time was one of the largest forensic examination units in all of Europe). *Id.* at 1.

<sup>2</sup> The number “10630-25-03” refers to the number used by the Taiwanese authorities to identify the seized devices. The “BRG” numbers referenced here refer to the numbering used by the government’s expert Andrew Crain from the Berkeley Research Group (“BRG”).

being forensically imaged on February 20, 2017. *Id.* at 15. MMT employee Yi-Leng Chen accessed the USB device on February 13, 2017 from 11:25 to 19:25 and reviewed files and folders on the device. *Id.*

6. **10630-25-12 (BRG012) Toshiba 500GB drive from HP Laptop:** Laptop **106030-25-12**, purportedly submitted by Huang Shu-han to Taichung District Prosecutor's Office on February 9, 2017, was accessed on February 13 and 14, 2017 before being forensically imaged on February 20, 2017. *Id.* at 16-17. MMT employee Yi-Leng Chen accessed the laptop on February 13, 2017 from 11:25 to 19:25 and reviewed files and folders on the device. *Id.* at 16.
7. **106030-25-13 (BRG013) PNY 3.0 128GB USB drive:** USB disk **106030-25-13**, purportedly submitted by Huang Shu-han to Taichung District Prosecutor's Office on February 9, 2017, was accessed on February 9, 13 and 14, 2017 before being forensically imaged on February 20, 2017. *Id.* at 17-18. MMT employee Yi-Leng Chen accessed the USB device on February 13, 2017 from 11:25 to 19:25 and reviewed files and folders on the device. *Id.*
8. **10630-25-14 (BRG014) Kingston Data Traveler 2.0 64GB USB drive:** USB disk **106030-25-14**, purportedly submitted by Huang Shu-han to Taichung District Prosecutor's Office on February 9, 2017, was accessed on February 13 and 14, 2017 before being forensically imaged on February 20, 2017. *Id.* at 18-19. MMT employee Yi-Leng Chen accessed the USB drive on February 13, 2017 from 11:25 to 19:25 and reviewed files and folders on the device. *Id.*
9. **10630-25-23 (BRG023) Kingston drive from Acer Laptop:** Laptop **106030-25-23**, seized on February 14, 2017, was accessed later on the same day. *Id.* at 19-20. 2,114 files or folders had their Modified, Accessed and Created time and date metadata information updated, including 1,369 files or folders that were created and 94 files or folders deleted on or after that date. *Id.* at 19. Of the files and folders added, 590 were added to the User Desktop under the folder NBD, this data originated from the UMC server \\p58f21data\. *Id.* at 20. The total data size of the added files is 2.1 Gigabytes. *Id.*
10. **10630-25-24 (BRG024) Transcend 32GB USB drive:** USB disk **106030-25-24**, seized on February 14, 2017, was accessed after seizure in the late afternoon on the same day. *Id.* at 20-21. 2,854 files or folders were created then with a total data size of more than 5.6 Gigabytes, which overwrote data and space and destroyed any evidence that existed thereon at the time of seizure by the MJIB. *Id.*

Despite clearly-established best practices requiring that seized devices be forensically imaged as soon as possible – and most importantly, before accessing any of the devices – the MJIB did not begin forensically imaging the seized devices until February 18, 2017 – eleven days after it had conducted the first raid of UMC facilities and at least four days since the last of the 26 devices was seized. Sloan Decl., Ex. D (Certificates Regarding the Forensic Image) at 12. The MJIB Lab completed the imaging process on February 21, 2017. *Id.* One of the devices seized turned out to

1 be damaged, therefore 25 devices were imaged. Sloan Decl., Ex. E (Certificate With Respect to  
 2 Seized Items) at 4. According to the documents produced by the Taiwanese authorities, the data  
 3 produced was saved in a 1 TB portable hard drive marked Exhibit 48. Sloan Decl., Ex. C (Evidence  
 4 Transfer Explanation) at 2.

5 B. DOJ's Request for Mutual Legal Assistance and Transfer of Evidentiary Materials

6 In November 2019, the Taichung District Court purportedly made a copy of the data stored  
 7 on Exhibit 48 on another 1 TB portable hard drive marked No. 106030 and provided it to a prosecutor  
 8 of the Taichung District Prosecutors Office. *Id.* at 3.

9 In December 2019, the Taiwan Ministry of Justice ("MOJ") received the 7th supplemental  
 10 request for assistance from the International Affairs Office of the United States Department of Justice  
 11 ("DOJ"). *Id.* The MOJ instructed the Taichung District Prosecutors Office to handle the request.  
 12 *Id.* Since the exhibits listed in the Taiwan indictment were in the custody of Taichung District court,  
 13 the Taichung District Prosecutors Office submitted requests to the Taichung District Court for  
 14 evidence in the court's custody but the requests were denied. *Id.*

15 In March 2020, the Taichung District Prosecutors Office reportedly made a copy of the data  
 16 stored on hard drive No. 106030 on a 1 TB portable hard drive and marked it No. 106030-copy. *Id.*  
 17 This hard drive was subsequently delivered to the Department of International and Cross-Strait Legal  
 18 Affairs of the MOJ. *Id.* Hard Drive No. 106030 was eventually delivered to the U.S. Sloan Decl.,  
 19 Ex. E (Certificate With Respect to Seized Items) at 4.

20 C. Discovery of Alleged Trade Secrets on Forensic Image of Seized Devices

21 By forensically investigating the forensic image of the seized devices, the government claims  
 22 to have located the alleged trade secrets alleged in the Indictment in this case (*see* ECF 1, ¶12(a)-  
 23 (h)(listing Alleged Trade Secrets Nos. 1-8) on devices 10630-25-03, 10630-25-08, 10630-25-09,  
 24 10630-25-10, 10630-25-11, 10630-25-13, 10630-25-14, 10630-25-26, and FTW-000158  
 25 (TUH194).<sup>3</sup> Sloan Decl., Ex. F (Andrew Crain Expert Report ("Crain Report")) at 6, FN 8. Of these  
 26 nine devices, however, six had been corrupted prior to their imaging, namely, Device 10630-25-03,  
 27

28 <sup>3</sup> FTW-000158 (TUH194) is purportedly JT Ho's UMC-issued laptop and was not one of the 26  
 devices seized in February 2017.

Device 10630-25-09, Device 10630-25-11, Device 10630-25-12, Device 10630-25-13, and Device 10630-25-14. Sloan Decl., Ex. G (Ashley Report) at 8-19.

Specifically, each of the alleged Trade Secrets is claimed to have been found in the following devices:

1. ***Trade Secret 1*** (16 documents)<sup>4</sup>

- (a) Device 10630-25-03, containing documents 6 and 10-16<sup>5</sup>;
- (b) Device 106030-25-08, containing documents 8 and 9<sup>6</sup>;
- (c) Device 106030-25-09, containing documents 2<sup>7</sup>, 3<sup>8</sup>, 6, and 8-16;
- (d) Device 106030-25-10, containing documents 8 and 9;
- (e) Device 106030-25-11, containing documents 2, 4-7<sup>9</sup>, and 10-16;
- (f) Device 106030-25-12, used to open documents 4-7 and 10-16;
- (g) Device 106030-25-13, containing documents 2, 3, 6, 8, 9, and 10-16;

<sup>4</sup> According to paragraph 4 of the United States' Bill of Particulars (Doc. 203) and the Crain Report, a total of 16 documents allegedly contain trade secret information designated under Trade Secret 1 in addition to Trade Secrets 2 through 8. Bill of Particulars at 2; Crain at 7-10.

<sup>5</sup> According to the Crain Report, documents 6 and 10-16 of Trade Secret 1 refer to the following documents: \$RZZ1XJM.xls, Rexchip 25nm Flowsummary 0614 Diff (version 1).xls, Rexchip%2025nm%20Flow%20summary%200614%20Diff, Rexchip 25nm Flow summary 0614 Diff.xls, Rexchip 25nm Flow summary \_IMP & RTP.xls, Rexchip 25nm Flow summary 0614 CMP.xls, Rexchip 25nm Flow summary 0614 Photo.xls, Rexchip 25nm Flow summary 0614 wet.xls, Rexchip 25nm Flow summary 0710 TF.xls. Sloan Decl., Ex. 6 (Crain Report) at 9.

<sup>6</sup> According to the Crain Report, documents 8 and 9 of Trade Secret 1 refer to R1 F72 1GC Flow0411 no defect.xls and R1 F721GC Flow0411 no defect\_1.xls. Sloan Decl., Ex. 6 (Crain Report) at 10.

<sup>7</sup> According to the Crain Report, document 2 of Trade Secret 1 refers to ★★Elpida 25nm process flow\_Modify.ppt. Sloan Decl., Ex. 6 (Crain Report) at 7.

<sup>8</sup> According to the Crain Report, document 3 of Trade Secret 1 refers to ★★Elpida 25nm process flow\_peri.ppt. Sloan Decl., Ex. 6 (Crain Report) at 8.

<sup>9</sup> According to the Crain Report, document 4 of Trade Secret 1 refers to dram\_comparison\_workshop\_100-110\_series.pdf and document 5 of Trade Secret 1 refers to Elpida 25nm process flow.pdf. Sloan Decl., Ex. 6 (Crain Report) at 8. Also, according to the Crain Report, document 7 of Trade Secret 1 refers to \$R29TV46.xlsb; originally named Template\_Tool Mapping\_Fab11\_Fab16 110sD Tool Risk (F16)-0831 discussion (version 1).xlsb, and various permutations of this filename. Sloan Decl., Ex. 6 (Crain Report) at 9.

1 (h) Device 106030-25-14, containing documents 4-7 and 10-16;

2 (i) Device 106030-25-26, containing documents 6 and 10-16;

3 (j) Device FTW-000157 (TUH193), used to open documents 6 and 10-  
4 16;

5 (k) Device FTW-000158 (TUH194), containing documents 4-7 and 10-  
6 16.

7 **2. Trade Secret 2**

8 (a) Device 10630-25-09;

9 (b) Device 106030-25-13;

10 (c) Device 106030-25-26.

11 **3. Trade Secret 3**

12 (a) Device 10630-25-09;

13 (b) Device 106030-25-13;

14 (c) Device 106030-25-26.

15 **4. Trade Secret 4**

16 (a) Device 10630-25-09;

17 (b) Device 106030-25-13;

18 (c) Device 106030-25-26.

19 **5. Trade Secret 5**

20 (a) Device 10630-25-03;

21 (b) Device 10630-25-09;

22 (c) Device 10630-25-12;

23 (d) Device 106030-25-13;

24 (e) Device 106030-25-26.

25 **6. Trade Secret 6**

26 (a) Device 10630-25-03;

27 (b) Device 10630-25-09;

28 (c) Device 10630-25-11;

(d) Device 10630-25-12 (used to access);

- (e) Device 106030-25-13;
- (f) Device 10630-25-14;
- (g) Device 106030-25-26;
- (h) FTW-000158 (TUH194).

**7. Trade Secret 7**

- (a) Device 10630-25-03;
- (b) Device 10630-25-09;
- (c) Device 10630-25-11;
- (d) Device 10630-25-12 (used to access);
- (e) Device 106030-25-13;
- (f) Device 10630-25-14;
- (g) Device 106030-25-26;
- (h) FTW-000158 (TUH194).

**8. Trade Secret 8**

- (a) Device 10630-25-09;
- (b) Device 10630-25-11;
- (c) Device 10630-25-12 (used to access);
- (d) Device 106030-25-13;
- (e) Device 10630-25-14;
- (f) Device 106030-25-26.

*See* Sloan Decl., Ex. F (Crain Report) at 7-13.

The government initiated the instant proceeding based largely on the electronic information that was improperly handled by the Taiwan authorities.

**III. ARGUMENT**

The Court should exclude the forensic image of the corrupted devices created by the MJIB Lab because the MJIB's post-seizure, pre-imaging access of said devices significantly corrupted and contaminated ten of the original devices. As a result, any forensic images generated by the MJIB can no longer reflect the data stored on those devices in "substantially the same condition" as when

1 they were seized. Therefore, the government cannot meet its burden to authenticate the forensic  
 2 images under Rule 901(a) of the Federal Rules of Evidence. In the alternative, the Court should  
 3 exclude said forensic image as a sanction against the government for spoliation of evidence.

4 Federal Rule of Evidence 104(a) permits the court to determine the admissibility of evidence  
 5 before trial. The forensic image may be admitted only if the court is satisfied by evidence sufficient  
 6 to support a finding that the forensic image is what the government claims it is. Fed. R. Evid. 901(a).  
 7 The key purpose of the authentication requirement is to ensure that only genuine and trustworthy  
 8 evidence is considered at trial. *See e.g., United States v. Panero*, 266 F.3d 939, 951 (9th Cir. 2001)  
 9 (holding for evidence to meet authenticity requirement, trial court must be satisfied that it is accurate,  
 10 authentic, and generally trustworthy). “It is of the utmost importance that, so far as practicalities  
 11 permit, there should not be a legitimate question about the integrity of physical evidence seized by  
 12 the government and introduced into evidence against an accused.” *United States v. Godoy*, 528 F.2d  
 13 281, 284 (9th Cir. 1975) (per curiam).

14 A. The Prosecution Has Not Produced Sufficient Evidence For A Reasonable Juror To  
 15 Determine That The Devices Are In Substantially The Same Condition As When  
They Were Seized

16 Although chain of custody<sup>10</sup> defects go to the weight of the evidence rather than its  
 17 admissibility, the government must demonstrate that the devices when imaged were in “substantially  
 18 the same condition as when the crime was committed.” *United States v. Hock Chee Koo*, 770 F.  
 19 Supp. 2d 1115, 1126 (D. Or. 2011) (citing *United States v. Dickerson*, 873 F.2d 1181, 1185 (9th Cir.  
 20 1988)). Federal Rule of Evidence 901 requires the government to eliminate not absolutely, but as a  
 21 matter of reasonable probability the possibility of misidentification and adulteration. *Id.* (internal  
 22 citation omitted).

23 In *Koo*, the district court held that a forensic image of a laptop may not be offered as evidence  
 24 of what was on the laptop prior to its seizure where after its seizure and before it was imaged, the  
 25 individual in possession of the laptop “periodically booted it up . . . looked around” “perusing its  
 26

27 <sup>10</sup> Chain of custody is a component of authentication. *See e.g., United States v. Salcido*, 506 F.3d  
 28 729, 733 (9th Cir. 2007) (“[T]he government properly authenticated the videos and images under  
 Rule 901 by presenting detailed evidence as to the chain of custody, specifically how the images  
 were retrieved from the defendant’s computers.”).

content over the course of two days,” and according to an expert, “accessed, altered, or deleted” over 1,000 files. 770 F. Supp. 2d at 1125. The court ruled that a forensic image of the hard drive from an employee’s company-issued laptop was inadmissible to prove its contents at the time it was confiscated by a supervisor because the supervisor booted the machine, accessed files, and allegedly altered content before turning over the laptop to the FBI for processing. *Id.* In reaching its holding, the court considered the expert’s testimony that the supervisor’s action in turning the computer on, moving a certain folder to the desktop and installing a data backup software altered the contents and data configuration of the laptop’s hard drive. *Id.* at 1125-26. As a result, “[t]here is no way that the data that resides in that [image] today is the same as it was when it was surrendered by [defendant].” *Id.* at 1126.

Here, the corrupted devices were accessed and their data altered between the time of seizure and the time of imaging. Moreover, a large volume of files was created, altered, or deleted on the following devices:

- **Device 10630-25-03:** Almost 35,000 files were added and more than 1,000 files were deleted. Sloan Decl., Ex. G (Ashley Report) at 11. Of the files and folders added, 32,688 were copied from the UMC server \\p58f21\Data\NBD on 2/7/2017. *Id.* The MJIB activity added 13.38 Gigabytes of data to the drive in total. *Id.*
- **Device 10630-25-04:** 93 files and 5 folders were created. *Id.*
- **Device 10630-25-09:** More than 4,500 files and folders had their metadata details altered with a number of files being added to or deleted. *Id.*
- **Device 10630-25-23:** 2,114 files or folders had their Modified, Accessed and Created time and date metadata information updated, including 1,369 files or folders that were created and 94 files or folders deleted on or after that date. Of the files and folders added, 590 were added to the User Desktop under the folder NBD, this data originated from the UMC server \\p58f21\data\\. The total data size of the added files is 2.1 Gigabytes. *Id.* at 19.
- **Device 10630-25-24:** 2,854 files or folders were created with a total data size of more than 5.6 Gigabytes. *Id.* at 20.

1 The evidence thus establishes that Exhibit 48, the forensic image of these devices delivered  
 2 to the United States by the Taiwanese authorities and produced to Jinhua in discovery, was not in  
 3 “substantially the same condition as when” the devices were originally seized by the MJIB, and these  
 4 forensic images should therefore be suppressed. *Koo*, 770 F. Supp. 2d at 1126 (internal citation  
 5 omitted).

6 The MJIB’s decision to give representatives from Micron, which had a strong motive to alter  
 7 information on the electronic devices, access to these devices before they were forensically imaged,  
 8 also calls into question the integrity of the data. *Koo*, 770 F. Supp. 2d at 1125 (giving weight to the  
 9 fact that the supervisor had filed a civil lawsuit against defendant the day before he obtained  
 10 defendant’s laptop). Here, Yi-Leng Chen, an MMT employee, accessed and reviewed files on seven  
 11 devices, including Device 10630-25-03, Device 10630-25-06, Device 10630-25-09, Device 10630-  
 12 25-11, Device 10630-25-12, Device 10630-25-13, and Device 10630-25-14. As an MMT employee,  
 13 Chen had a potential incentive to change information stored on the devices because it was MMT’s  
 14 and Micron’s filing of a criminal complaint with the Taiwanese authorities that led to the  
 15 investigation and raids on MMT’s competitor, UMC and its employees.

16 B. The Taiwan MJIB Failed To Follow Proper Forensic Protocol In Searching The  
 17 Seized Devices, Thereby Contaminating The Data That They Contain

18 It is well-established among forensic experts that the forensic image of any electronic devices  
 19 should be made immediately after the device is surrendered or seized. *See, e.g., United States v.*  
 20 *Rodriguez*, No. 16-CR-41G, 2018 WL 947266, at \*6 (W.D.N.Y. Feb. 20, 2018) (noting that this is  
 21 “a widespread, best practice with electronic discovery”) (citations omitted). As explained by  
 22 Jinhua’s computer forensics expert, John Ashley:

23 At the earliest opportunity after the seizure of such devices, verified forensic  
 24 images should be created on new or previously prepared media, with write  
 25 blocking devices utilized to prevent any possibility of data alteration or corruption  
 on the original devices. To avoid alteration or corruption of the evidence, all  
 investigation should be performed on verified copies of the forensic images, not  
 on the original devices.

26 Sloan Decl. Ex. G (Ashley Report) at 6.

27 Accordingly, because “the extraction of specific data files to some other medium can alter,  
 28 omit, or even destroy portions of the information contained in the original storage medium,”

1 “[p]reservation of the original medium or a complete mirror may ... be necessary in order to  
 2 safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial.”  
 3 *United States v. Ganas*, 824 F.3d 199, 215 (2d Cir. 2016). Moreover, retention of the original  
 4 storage medium or its mirror may be necessary to afford criminal defendants the opportunity to  
 5 challenge the authenticity or reliability of evidence allegedly retrieved with the help of their own  
 6 forensic experts. *Id.* (citing *United States v. Kimoto*, 588 F.3d 464, 480 (7th Cir. 2009)).

7       The necessity to preserve the original medium is also well recognized in scholarly writings  
 8 and practice handbooks. *See e.g.*, Eoghan Casey, *Digital Evidence and Computer Crime* 60 (3d ed.  
 9 2011) (“To demonstrate that digital evidence is authentic, it is generally necessary to satisfy the court  
 10 that it was acquired from a specific computer and/or location, that a complete and accurate copy of  
 11 digital evidence was acquired, and that it has remained unchanged since it was collected.”); Alan  
 12 Bush & Lee Winkelman, *People Problems in Deals*, 34 Corp. Couns. Rev. 125, 148 (2015) (“The  
 13 starting point for a forensic analysis is to perform a clean mirror image of the departed employee’s  
 14 hard drive. The image should be taken as soon as possible after any key employee has left and ceased  
 15 using the computer. . . . Using a computer before it is imaged jeopardizes the investigation. . . . Even  
 16 poking around the computer for a couple days to investigate for signs of data theft can spoil the  
 17 forensic trail.”); Manual for Complex Litigation, Fourth §11.446 (2004) (“Accuracy may be impaired  
 18 by incomplete data entry, mistakes in output instructions, programming errors, damage and  
 19 contamination of storage media, power outages, and equipment malfunctions. The integrity of data  
 20 may also be compromised in the course of discovery by improper search and retrieval techniques,  
 21 data conversion, or mishandling. The proponent of computerized evidence has the burden of laying  
 22 a proper foundation by establishing its accuracy.”); Daniel B. Garrie, *Plugged In: Guidebook to*  
 23 *Software and the Law*, § 6:5 Seven phases of forensic examination—Phase 2: Evidence acquisition  
 24 (2020) (“It is important to maintain the integrity of the information on the device, as any change in  
 25 the information can have implications on the final evidence presented at trial . . .”).

26       Here, in blatant disregard of these best practices, the Taiwan MJIB “(1) failed to create proper  
 27 forensic images of the devices immediately after they were seized; (2) performed searches or  
 28 otherwise accessed the subject devices after they were seized (rather than conducting all

1 investigations on the forensic images), thus altering and corrupting this evidence; and (3) in some  
 2 cases, added information onto these devices, thus further corrupting the evidence.” Sloan Decl., Ex.  
 3 G (Ashley Report) at 7. Therefore, the forensic images of the seized devices must be excluded in  
 4 their entirety because the government cannot establish that the subject data is in “substantially the  
 5 same condition as when the crime was committed” or when the devices were seized, as required by  
 6 Fed. R. Evid. 901. *See Koo*, 770 F. Supp. 2d at 1126.

7 C. The Government and its Taiwanese Counterpart Have Spoliated the Most Critical  
 8 Evidence for Both the Prosecution and the Defense by Negligently Handling the  
 9 Corrupted Devices Before Creating a Forensic Image.

10 Alternatively, the Court should exclude the forensic image of the corrupted devices because  
 11 they have been spoliated by the United States and its Taiwanese counterparts in the MJIB. The Court  
 12 has the inherent discretionary power to make appropriate evidentiary rulings in response to the  
 13 spoliation of relevant evidence, including the power to order their exclusion. *Glover v. BC Corp.*, 6  
 14 F.3d 1318, 1329 (9th Cir. 1993) (citing *Unigard Sec. Ins. Co. v. Lakewood Eng’g & Mfg. Corp.*, 982  
 15 F.2d 363, 368 (9th Cir. 1992)); *see California v. Trombetta*, 467 U.S. 479, 482–83, 104 S. Ct. 2528,  
 16 2530–31 (1984) (considering the suppression of breath-analysis tests results on the ground that the  
 17 arresting officers had failed to preserve the breath samples used in the test). A court may impose  
 18 sanctions against a party which is on notice that documents and information in its possession are  
 19 relevant to and reasonably calculated to lead to the discovery of admissible evidence, but destroys  
 20 such documents and information. *United States v. Maxxam, Inc.*, No. C-06-07497CWJCS, 2009 WL  
 21 817264, at \*7 (N.D. Cal. Mar. 27, 2009) (citation omitted). Bad faith is not required for spoliation  
 22 sanctions. *United States v. Safeco Ins. Co. of Am.*, No. 3:14-CV-00190-BLW, 2016 WL 901608, at  
 23 \*7 (D. Idaho Mar. 9, 2016) (citation omitted).

24 To establish a case of spoliation, Jinhua has to prove the following elements by a  
 25 preponderance of the evidence: (1) the government and its Taiwanese counterpart had an obligation  
 26 to preserve the corrupted devices when they were altered; (2) the destruction or loss was  
 27 accompanied by a ‘culpable state of mind;’ and (3) the evidence that was altered was relevant to the  
 28 defenses of Jinhua. *See Singleton v. Kernan*, No. 3:16-CV-2462-BAS-NLS, 2018 WL 5761688, at  
 \*2 (S.D. Cal. Nov. 1, 2018).

1. The significance of the information stored on the corrupted devices should have been obvious to the Taiwanese MJIB and they have acted in bad faith by deviating from the standard practice of immediately creating forensic images of the electronic devices upon seizure.

The government and the Taiwanese authorities knew they had to preserve the status quo of all the seized electronic devices for they are the source of the alleged trade secrets that are the basis for both the Taiwanese and U.S. criminal cases. Federal courts have recognized a duty to preserve evidence when a party knows or reasonably should know the evidence is relevant and would be prejudicial for an opposing party if the evidence is destroyed. *Singleton*, 2018 WL 5761688, at \*3 (citation omitted). Where a party has some notice that the evidence was potentially relevant to the litigation before it was destroyed, such destruction of evidence amounts to willful spoliation. *Id.* (citation omitted); *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, 167 F.R.D. 90, 112 (D. Colo. 1996) (criticizing a party for doing a “file by file” backup of certain device instead of making a forensic image which resulted in the loss of information and finding that the party “had a duty to utilize the method which would yield the most complete and accurate results.”).

In addition, although there is no “absolute duty to retain and to preserve all material that might be of conceivable evidentiary significance in a particular prosecution” on the part of the government, courts will recognize such a duty if the defendant establishes bad faith by the government in spoliating potential evidence. *See Arizona v. Youngblood*, 488 U.S. 51, 58, 109 S. Ct. 333, 337 (1988). Officers act in bad faith when they deviate from normal practice and display animus towards the defendant.

Here, the significance and evidentiary value of the seized devices is undeniable—both the government and the defendants rely on their contents to show or dispute the existence of trade secret information which forms the basis of this proceeding. The Taiwanese MJIB knew from the moment it raided UMC’s facilities in February 2017 that it was searching for trade secret information that purportedly belonged to Micron or MMT, and that this could lead to both civil litigation and criminal prosecutions in Taiwan and potentially the United States. Sloan Decl., Ex. A (Taiwan Indictment) at 7, 17. Moreover, the Taiwanese MJIB acted in bad faith by breaching the “widespread, best practice with electronic discovery” which demanded the creation of a forensic image before searching seized electronic devices. *See California v. Trombetta*, 467 U.S. at 488; *Rodriguez*, 2018

1 WL 947266, at \*6. Animus towards Jinhua and bad faith were also evident from the fact that the  
 2 forensic officers not only used key words provided by MMT, the claimant in the Taiwan Indictment,  
 3 to search for data on the seized devices, they actually invited an employee of MMT, who stood to  
 4 benefit from charges being brought against UMC and Jinhua, to review the seized devices before  
 5 they were forensically imaged. Sloan Decl., Ex. E (Certificate With Respect to Seized Items) at 5,  
 6 Ex. E (Ashley Report) at 8-17.

7 Accordingly, the MJIB and its counterparts in the U.S. DOJ had a duty to preserve the seized  
 8 electronic devices and the forensic evidence contained thereon in the same condition as when they  
 9 were seized. *See Nova Measuring Instruments Ltd. v. Nanometrics, Inc.*, 417 F. Supp. 2d 1121, 1122  
 10 (N.D. Cal. 2006) (requiring documents to be produced in their native format with original metadata)  
 11 (citation omitted); *In re Vioxx Prod. Liab. Litig.*, No. MDL 1657, 2005 WL 756742, at \*3 (E.D. La.  
 12 Feb. 18, 2005) (imposing the duty to preserve metadata information on the parties in pretrial order).

13 2. The Taiwanese authorities were at least negligent in deviating from the  
 14 established best practice of forensically imaging the corrupted devices  
immediately after they were seized and delivered to the MJIB Lab.

15 To establish that the party destroyed the evidence with a “culpable state of mind,” it is  
 16 sufficient to show that such party acted with negligence. *Singleton*, 2018 WL 5761688, at \*4  
 17 (citation omitted). Although a finding of “bad faith” is not a prerequisite for this element, if shown,  
 18 bad faith automatically establishes relevance, the third element of the test. *Id.* at \*2, 4. (citing Glover,  
 19 6 F.3d at 1329). By contract, if the destruction is merely negligent, the party seeking sanctions must  
 20 prove that the deleted or altered evidence was relevant. *Id.* at 2 (finding plaintiff has satisfied the  
 21 burden of showing a culpable state of mind through negligent loss of the documents when defendants  
 22 do not argue that the record was destroyed pursuant to normal business practices in accordance with  
 23 the document retention policies).

24 Under the facts presented here, the Taiwanese authorities were at least negligent in not  
 25 following the “widespread, best practice with electronic discovery,” which requires immediately  
 26 creating the forensic image of electronic devices after seizure. *Rodriguez*, 2018 WL 947266, at \*6;  
 27 *supra* Section III B. The seized devices were immediately delivered to the MJIB Lab, which was  
 28 capable of forensically imaging the devices, after they were seized. Sloan Decl., Ex. B (Chen

Description) at 1. Rather than creating a forensic image right away, however, the Taiwanese authorities ran searches on the corrupted devices, contaminating their data. Sloan Decl., Ex. G (Ashley Report) at 7. As a result, thousands of new files were created on the corrupted devices, the metadata of those devices was altered, and “[g]igabytes of electronic data storage space were overwritten and are no longer available to be investigated.” Sloan Decl., Ex. G (Ashley Report) at 7-21. Therefore, the government and its Taiwanese counterpart have negligently caused the spoliation of the corrupted devices.

3. The corrupted devices in their untampered original state would have been the most relevant and crucial evidence on the issue of whether alleged trade secret information were in the possession of the defendants.

Finally, the status quo of the corrupted devices at the time they were seized is arguably the most important evidence in this action. As discussed above, the MJIB’s and the United States’ cases against the defendants rests almost exclusively upon the alleged Trade Secret information found on the corrupted devices.<sup>11</sup> Without such evidence, the government’s case will wither. Because the forensic images of these devices have been corrupted, Jinhua is left to work with incomplete and contaminated information.

Accordingly, since admitting the forensic image of the corrupted devices would unfairly prejudice Jinhua, the Court should exclude it from the evidence. *See Caruso v. Solorio*, No. 115CV780AWIEPGPC, 2021 WL 3514610, at \*9 (E.D. Cal. Aug. 10, 2021) (citing *Unigard Sec. Ins. Co.*, 982 F.2d at 368) (providing that preclusion of evidence is a proper sanction when the admission of spoliated evidence would unfairly prejudice an opposing party).

#### IV. CONCLUSION

For the foregoing reasons, Jinhua moves this Court for an order excluding the forensic image of the corrupted devices from admission into evidence.

---

<sup>11</sup> Significantly, however, the Taiwanese authorities did not bring any charges against Jinhua or Stephen Chen. *See* Sloan Decl., Ex. A at 1.

1 Dated: December 1, 2021      Respectfully submitted,

2 SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

3  
4 By:                   /s/ Matthew E. Sloan                    
5 MATTHEW E. SLOAN  
6 Attorneys for Defendant  
7 FUJIAN JINHUA INTEGRATED CIRCUIT CO., LTD.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28